REMARKS

Claims 1-12 are pending in the Application. Claims 1-12 are provisionally rejected on the ground of non-statutory obviousness-type double patenting. Claims 1-3, 5-7 and 9-11 are rejected under 35 U.S.C. §102(e). Claims 4, 8 and 12 are rejected under 35 U.S.C. §103(a). Applicants respectfully traverse these rejections for at least the reasons stated below and respectfully request that the Examiner reconsider and withdraw these rejections.

I. PROVISIONAL REJECTION UNDER OBVIOUSNESS-TYPE DOUBLE PATENTING:

The Examiner has provisionally rejected claims 1-12 under the judicially created doctrine of obviousness-type double patenting in view of co-pending Application No. 10/749,584 and in view of co-pending Application No. 10/994,620. Applicants note that if the "provisional" double patenting rejection is the only rejection remaining in an application (either the present application or in Application No. 10/749,584 or in Application No. 10/994,620), then the Examiner should withdraw the rejection and permit that application to issue as a patent. M.P.E.P. §804. The "provisional" double patenting rejection may then be converted into a double patenting rejection in the other application at the time the one application issues as a patent. M.P.E.P. §804.

II. REJECTIONS UNDER 35 U.S.C. §102(e):

The Examiner has rejected claims 1-3, 5-7 and 9-11 under 35 U.S.C. §102(e) as being anticipated Thompson et al. (U.S. Patent No. 6,725,382) (hereinafter "Thompson"). Applicants respectfully traverse these rejections for at least the reasons stated below and respectfully request the Examiner to reconsider and withdraw these rejections.

For a claim to be anticipated under 35 U.S.C. §102, each and every claim limitation must be found within the cited prior art reference and arranged as required by the claim. M.P.E.P. §2131.

Regarding claims 1, 5 and 9, Applicants respectfully assert that Thompson does not disclose "providing protected storage accessible only by Basic Input Output System (BIOS) code." The Examiner cites column 3, lines 10-26 and 47-57 as well as Figure 3 of Thompson as disclosing the above-cited claim limitation. Office Action (4/21/2006), page 5. Applicants respectfully traverse and assert that Thompson instead discloses a personal computer 100 that has a storage element like BIOS device 108: one whose contents cannot be easily accessed or bypassed by a user of the device while operation of the device is disabled, and whose operability hinges on those contents. Column 3, lines 21-26. Thompson further discloses that the BIOS device contains a security program 302 including an encryption key 304 and password 306 entries. Column 3, lines 51-53. Hence, Thompson discloses that a personal computer includes a BIOS device that contains a security program. The BIOS device (element 108) of Thompson is not a protected storage accessible only by BIOS code. There is no language in the cited passages that discloses that the BIOS device (element 108) of Thompson is accessible only by the BIOS code. Thus, Thompson does not disclose all of the limitations of claims 1, 5 and 9, and thus Thompson does not anticipate claims 1, 5 and 9. M.P.E.P. §2131.

Furthermore, regarding claims 1, 5 and 9, Applicants respectfully assert that Thompson does not disclose "encrypting normally unaccessible (NA) data with said symmetrical encryption key." The Examiner cites column 3, lines 47-57 and item 306 of Figure 3 of Thompson as disclosing the above-cited claim limitation. Office Action (4/21/2006), page 5. Applicants respectfully traverse and assert that Thompson instead discloses that the BIOS device 108 contains a security program 302 including an encryption key 304 and password 306 entries. Column 3, lines 51-53. There is no language in the cited passage that discloses that the password 306 (Examiner asserts that password 306 discloses the claimed NA data) is encrypted using the encryption key 304 (Examiner asserts that the encryption key 304 discloses the claimed symmetrical encryption key). Hence, Thompson does not disclose encrypting NA data with a symmetrical encryption key. Thus, Thompson does not disclose all of the limitations of claims 1, 5 and 9, and thus Thompson does not anticipate claims 1, 5 and 9. M.P.E.P. §2131.

Further, the Examiner has not provided any basis in fact and/or technical reasoning to support the assertion that password entries 306 of Thompson are equivalent to "normally unaccessible data." The Examiner must provide a basis in fact and/or technical reasoning to support the assertion that password entries 306, as disclosed in Thompson, is the same as "normally unaccessible data." *Ex parte Levy*, 17 U.S.P.Q.2d 1461, 1464 (Bd. Pat. App. & Inter. 1990). That is, the Examiner must provide extrinsic evidence that must make clear that password entries 306, as disclosed in Thompson, is the same as "normally unaccessible data," and that it would be so recognized by persons of ordinary skill. *In re Robertson*, 169 F.3d 743, 745 (Fed. Cir. 1999). Since the Examiner has not provided any such objective evidence, the Examiner has not presented a *prima facie* case of anticipation in rejecting claims 1, 5 and 9. M.P.E.P. §2131.

Additionally, regarding claims 1, 5 and 9, Applicants respectfully assert that Thompson does not disclose "storing said encrypted NA data and accessible non-encrypted (ANE) data in an unprotected electronically erasable programmable read only memory (EEPROM) with existing write protect algorithms." The Examiner cites column 3, line 27 – column 4, line 5 of Thompson as disclosing the above-cited claim limitation. Office Action (4/21/2006), page 5. The Examiner further asserts that write protected algorithms are inherently required in order for the data stored in the EEPROM to be erased. Office Action (4/21/2006), page 5. Applicants respectfully traverse.

Thompson instead discloses that BIOS device 108 comprises non-volatile, "permanent", memory, one whose contents are preserved even when power is absent. Column 3, lines 28-30. Thompson further discloses that unlike ROM 104, however, it is electrically alterable and programmable under control of special software, in order to update BIOS over the life of PC 100. Column 3, lines 30-32. Additionally, Thompson discloses that storage devices of this type are known as programmable read-only memory (PROM), electrically-erasable PROM (EEPROM), or flash memory. Column 3, lines 33-35. Hence, Thompson discloses that BIOS device 108 (Examiner has previously asserted that BIOS device 108 disclosed the claimed protected storage) may be a storage device that is EEPROM. The Examiner cannot cite the same element (BIOS device 108) as disclosing both a protected storage and an unprotected EEPROM. Based on the doctrine of claim differentiation, these claim elements are separate elements and the Examiner must cite to separate elements in Thompson as allegedly disclosing these elements. Thus, Thompson does not disclose all of the limitations of claims 1, 5 and 9, and thus Thompson does not anticipate claims 1, 5 and 9. M.P.E.P. §2131.

Further, there is no language in the cited passage that discloses storing encrypted NA data in an unprotected EEPROM. Instead, the Examiner asserts that BIOS device 108 of Thompson is a protected storage unit since it contains a security program. Neither is there any language in the cited passage that discloses storing accessible non-encrypted data in an unprotected EEPROM. Neither is there any language in the cited passage that discloses storing the encrypted NA data and accessible non-encrypted (ANE) data in an unprotected electronically erasable programmable read only memory (EEPROM) with existing write protect algorithms. Thus, Thompson does not disclose all of the limitations of claims 1, 5 and 9, and thus Thompson does not anticipate claims 1, 5 and 9. M.P.E.P. §2131.

Further, Applicants respectfully traverse the assertion that write protect algorithms are inherently disclosed in Thompson. The Examiner has not pointed to any language in Thompson that BIOS device 108 is an EEPROM that needs a write protected algorithm to erase the stored data. The Examiner must provide a basis in fact and/or technical reasoning to support the assertion that Thompson inherently discloses write protect algorithms. *Ex parte Levy*, 17 U.S.P.Q.2d 1461, 1464 (Bd. Pat. App. & Inter. 1990). That is, the Examiner must provide extrinsic evidence that must make clear that Thompson inherently discloses write protect algorithms, and that it would be so recognized by persons of ordinary skill. *In re Robertson*, 169 F.3d 743, 745 (Fed. Cir. 1999). Since the Examiner has not provided any such objective evidence, the Examiner has not presented a *prima facie* case of anticipation in rejecting claims 1, 5 and 9. M.P.E.P. §2131.

Claims 2-3 each recite combinations of features of independent claim 1 and hence are not anticipated by Thompson for at least the reasons that claim 1 is not anticipated by Thompson. Claims 6-7 each recite combinations of features of independent claim 5 and hence are not anticipated by Thompson for at least the reasons that claim 5 is not anticipated by Thompson. Claims 10-11 each recite combinations of features of independent claim 9 and hence are not anticipated by Thompson for at least the reasons that claim 9 is not anticipated by Thompson.

Regarding claims 2, 6 and 10, Applicants respectfully assert that Thompson does not disclose "altering said ANE data by issuing an existing write request to said BIOS from said write protect algorithms for said EEPROM; and updating said ANE data in said EEPROM." The Examiner cites column 3, lines 27-46 and column 7, lines 26-44 of Thompson as disclosing the above-cited claim limitation. Office Action (4/21/2006), page 6. Applicants respectfully traverse.

Thompson instead discloses that BIOS device 108 comprises non-volatile, permanent, memory, one whose contents are preserved even when power is absent. Column 3, lines 38-30. Thompson further discloses that CPU 102 stores the new encrypted password as password 306 in BIOS device 108. Column 7, lines 30-31. Thompson additionally discloses that CPU 102 also stores it in memory 254 of security card 250 in place of any previously stored contents therein. Column 7, lines 31-33. Thompson further discloses that security card 250 may need to supply the entire BIOS service 108 contents along with the new password 308. Column 7, lines 34-36. Hence, Thompson discloses storing an <u>encrypted</u> password in both the BIOS device and in the memory 254 of security card 250. This is not the same as altering or updating accessible <u>non-encrypted</u> (ANE) data. Further, there is no language in the cited passage that discloses <u>altering ANE data</u>. Neither is there any language in the cited passage that discloses altering ANE data by issuing an existing write request to the BIOS. Neither is there any language in the cited passage that discloses altering ANE data by issuing an existing write request to the BIOS from the write protect algorithms for the EEPROM. Neither is there any language in the cited passage that discloses updating the ANE data in the EEPROM. Thus, Thompson does not disclose all of the limitations of claims 2, 6 and 10, and thus Thompson does not anticipate claims 2, 6 and 10. M.P.E.P. §2131.

Regarding claims 3, 7 and 11, Applicants respectfully assert that Thompson does not disclose "accessing said NA data via a change request issued to said BIOS over a secure communication link; validating said change request." The Examiner cites column 5, line 45 – column 6, line 67 and item 130 of Figure 1 of Thompson as disclosing the above-cited claim limitations. Office Action (4/21/2006), page 6. Applicants respectfully traverse and assert that Thompson instead discloses that if the user elects to change the password or elects to establish a password, then CPU 102 proceeds to interact with either TCA 150 or security card 250. Column 5, lines 46-50. Thompson further discloses that item 130 of Figure 1 corresponds to a data network 130. Column 5, lines 51-52. There is no language in the cited passage that discloses accessing NA data via a change request issued to the BIOS. Neither is there any language in the cited passage that discloses accessing NA data via a change request issued to the BIOS over a secure communication link. Neither is there any language in the cited passage that discloses validating the change request. Thus, Thompson does not disclose all of the limitations of claims 3, 7 and 11, and thus Thompson does not anticipate claims 3, 7 and 11. M.P.E.P. §2131.

Furthermore, regarding claims 3, 7 and 11, Applicants respectfully assert that Thompson does not disclose "retrieving said symmetrical encryption key by said BIOS in response to said validated change request; using said symmetrical encryption key to decrypt and alter said NA data; encrypting said altered NA data using said symmetrical encryption key; and storing said altered encrypted NA data in said EEPROM." The Examiner cites column 3, lines 27-46 and column 7, lines 25-44 of Thompson as disclosing the above-cited claim limitations. Office Action (4/21/2006), page 6. Applicants respectfully traverse.

Thompson instead discloses that BIOS device 108 comprises non-volatile, permanent, memory, one whose contents are preserved even when power is absent. Column 3, lines 38-30. Thompson further discloses that CPU 102 stores the new encrypted password as password 306 in BIOS device 108. Column 7, lines 30-31. Thompson additionally discloses that CPU 102 also stores it in memory 254 of security card 250 in place of any previously stored contents therein. Column 7, lines 31-33. Thompson further discloses that security card 250 may need to supply the entire BIOS service 108 contents along with the new password 308. Column 7, lines 34-36. Hence, Thompson discloses storing an encrypted password in both the BIOS device and in the memory 254 of security card 250.

There is no language in the cited passages that discloses retrieving the symmetrical encryption key by the BIOS in response to a validated change request. Neither is there any language in the cited passages that discloses using a symmetrical encryption key to decrypt and alter the NA data. Neither is there any language in the cited passages that discloses encrypting the altered NA data using the symmetrical encryption key. Neither is there any language in the cited passages that discloses storing the altered encrypted NA data in the EEPROM. Thus, Thompson does not disclose all of the limitations of claims 3, 7 and 11, and thus Thompson does not anticipate claims 3, 7 and 11. M.P.E.P. §2131.

As a result of the foregoing, Applicants respectfully assert that not each and every claim limitation was found within Thompson, and thus claims 1-3, 5-7 and 9-11 are not anticipated by Thompson. M.P.E.P. §2131.

III. REJECTIONS UNDER 35 U.S.C. §103(a):

The Examiner has rejected claims 4, 8 and 12 under 35 U.S.C. §103(a) as being unpatentable over Thompson in view of Mirov et al. (U.S. Patent No. 6,138,236) (hereinafter "Mirov"). Applicants respectfully traverse these rejections for at least the reasons stated below and respectfully request the Examiner to reconsider and withdraw these rejections.

A. Thompson and Mirov, taken singly or in combination, do not teach or suggest the following claim limitations.

Regarding claims 4, 8 and 12, Applicants respectfully assert that Thompson and Mirov, taken singly or in combination, do not teach or suggest "hashing said ANE data and encrypting said hash with said symmetrical encryption key; storing said encrypted hash with said ANE data; computing a hash of configuration data in said ANE data on a boot-up request; decrypting said stored encrypted hash of said configuration data; comparing said decrypted hash of said stored configuration data to said computed hash of said configuration data from said ANE data; booting normally in response to a compare of said decrypted hash and said computed hash; and issuing tamper notification and initiating recovery processes on a non-compare of said decrypted hash and said computed hash." The Examiner cites column 2, lines 21-32 and column 3, line 55 – column 5, line 50 of Mirov as teaching the above-cited claim limitation. Office Action (4/21/2006), page 7. Applicants respectfully traverse.

Mirov instead teaches a computer system where a portion of code/data stored in a non-volatile memory device can be dynamically modified or updated without removing any covers or parts from the computer system. Column 2, lines 17-20. Mirov further teaches that the computer system of the preferred embodiment includes a flash memory component coupled to the bus for storing non-volatile code and data. Column 2, lines 33-34. Mirov further teaches that using the present invention, the contents of the flash memory may be replaced, modified, updated or reprogrammed without the need for removing and/or replacing any computer system hardware components. Column 2, lines 36-40.

There is no language in the cited passages that teaches hashing ANE data. Neither is there any language in the cited passages that teaches hashing ANE data and encrypting the hash with a symmetrical encryption key. Neither is there any language in the cited passages that teaches storing an encrypted hash. Neither is there any language in the cited passages that teaches storing an encrypted hash with the ANE data. Neither is there any language in the cited passages that teaches computing a hash of configuration data. Neither is there any language in the cited passages that teaches computing a hash of configuration data in the ANE data. Neither is there any language in the cited passages that teaches computing a hash of configuration data in the ANE data on a boot-up request. Neither is there any language in the cited passages that teaches decrypting the stored encrypted hash of the configuration data. Neither is there any language in the cited passages that teaches comparing the decrypted hash of the stored configuration data to the computed hash of the configuration data from the ANE data. Neither is there any language in the cited passages that teaches booting normally in response to a compare of the decrypted hash and the computed hash. Neither is there any language in the cited passages that teaches issuing tamper notification. Neither is there any language in the cited passages that teaches issuing tamper notification and initiating recovery processes. Neither is there any language in the cited passages that teaches issuing tamper notification and initiating recovery processes on a non-compare of the decrypted hash and the computed hash. Therefore, the Examiner has not presented a *prima facie* case of obviousness in rejecting claims 4, 8 and 12, since the Examiner is relying upon incorrect, factual predicates in support of the rejections. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1455 (Fed. Cir. 1998).

B. Examiner's motivation for modifying Thompson with Mirov to incorporate the missing claim limitations of claims 4, 8 and 12 is insufficient.

Most if not all inventions arise from a combination of old elements. *See In re Rouffet*, 47 U.S.P.Q.2d 1453, 1457 (Fed. Cir. 1998). Obviousness is determined from the vantage point of a hypothetical person having ordinary skill in the art to which the patent pertains. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1457 (Fed. Cir. 1998). Therefore, an Examiner may often find every element of a claimed invention in the prior art. *Id.* However, identification in the prior art of each individual part claimed is insufficient to defeat patentability of the whole claimed invention. *See Id.* In order to establish a *prima facie* case of obviousness, the Examiner must show reasons that the skilled artisan, confronted with the same problems as the inventor and with no knowledge of the claimed invention, would select the elements from the cited prior art references for combination in the manner claimed. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1458 (Fed. Cir. 1998). That is, the Examiner must provide some suggestion or motivation, either in the references themselves, the knowledge of one of ordinary skill in the art, or, in some case, the nature of the problem to be solved, to modify the reference or to combine reference teachings. *See In re Dembiczak*, 175 F.3d 994, 999, 50 U.S.P.Q.2d 1614, 1617 (Fed. Cir. 1999). Whether the Examiner relies on an express or an implicit showing, the Examiner must provide particular findings related thereto. *In re Kotzab*, 55 U.S.P.Q.2d 1313, 1317 (Fed. Cir. 2000).

The Examiner admits that Thompson does not teach the limitations of claims 4, 8 and 12. Office Action (4/21/2006), page 7. The Examiner modifies Thompson with Mirov to include the limitations of claims 4, 8 and 12 in order "to authenticate plurality of micro-code to authorize execution of micro-code to ensure the integrity of the stored data." Office Action (4/21/2006), page 7. The Examiner's motivation is insufficient to establish a *prima facie* case of obviousness in rejecting claims 4, 8 and 12.

The Examiner has not provided a source for his motivation for modifying Thompson to include the limitations of claims 4, 8 and 12. The Examiner simply states "to authenticate plurality of micro-code to authorize execution of micro-code to ensure the integrity of the stored data" as motivation for modifying Thompson to include the limitations of claims 4, 8 and 12. The motivation to modify Thompson must come from one of three possible sources: the nature of the problem to be solved, the teachings of the prior art, and the knowledge of persons of ordinary skill in the art. *In re Rouffet*, 149 F.3d 1350, 1357, 47 U.S.P.Q.2d 1453, 1457-48 (Fed. Cir. 1998). The Examiner has not provided any evidence that his motivation comes from any of these sources. Instead, the Examiner is relying upon his own subjective opinion which is insufficient to support a *prima facie* case of obviousness. *In re Lee*, 61 U.S.P.Q.2d 1430, 1434 (Fed. Cir. 2002). Consequently, the Examiner's motivation is insufficient to support a *prima facie* case of obviousness for rejecting claims 4, 8 and 12. *Id.*

Further, the Examiner's motivation ("to authenticate plurality of micro-code to authorize execution of micro-code to ensure the integrity of the stored data") does not provide reasons, as discussed further below, that the skilled artisan, confronted with the same problems as the inventor and with no knowledge of the claimed invention, would modify Thompson to include the missing claim limitations of claims 4, 8 and 12. Accordingly, the Examiner has not presented a *prima facie* case of obviousness for rejecting claims 4, 8 and 12. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1458 (Fed. Cir. 1998).

Thompson addresses the problem of providing a security mechanism in a portable computer for thwarting theft or unauthorized access while making it easy to deal with lost passwords and validation of the device by some authority. Column 1, lines 25-48. The Examiner has not provided any reasons as to why one skilled in the art would modify Thompson, which teaches providing a security mechanism in a portable computer for thwarting theft or unauthorized access while making it easy to deal with lost passwords and validation of the device by some authority, to (1) hash ANE data and encrypt the hash with an symmetrical encryption key; (2) store the encrypted hash with the ANE data; (3) compute a hash of configuration data in the ANE data on a boot-up request; (4) decrypt the stored encrypted hash of the configuration data; (5) compare the decrypted hash of the stored configuration data to the computed hash of the configuration data from the ANE data; (6) boot normally in response to a compare of the decrypted hash and the computed hash; and (7) issue tamper notification and initiate recovery processes on a non-compare of the decrypted hash and the computed hash (missing claim limitations of Thompson). The Examiner's motivation ("to authenticate plurality of micro-code to authorize execution of micro-code to ensure the integrity of the stored data") does not provide such reasoning. Further, the Examiner has not explained how authenticating a plurality of micro-code to authorize execution of micro-code to ensure the integrity of the stored data (Examiner's motivation) relates to the limitations of claims 4, 8 and 12. Hence, the Examiner's motivation does not provide reasons that the skilled artisan, confronted with the same problems as the inventor and with no knowledge of the claimed invention, would modify Thompson to include the missing claim limitations of claims 4, 8 and 12. Accordingly, the Examiner has not presented a *prima facie* case of obviousness for rejecting claims 4, 8 and 12. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1458 (Fed. Cir. 1998).

IV. CONCLUSION:

As a result of the foregoing, it is asserted by Applicants that claims 1-12 in the Application are in condition for allowance, and Applicants respectfully request an allowance of such claims. Applicants respectfully request that the Examiner call Applicants' attorney at the below listed number if the Examiner believes that such a discussion would be helpful in resolving any remaining issues.

Respectfully submitted,

WINSTEAD SECHREST & MINICK P.C.

Attorneys for Applicants

By:____________________
Robert A. Voigt, Jr.
Reg. No. 47,159

P.O. Box 50784
Dallas, TX 75201
(512) 370-2832

Austin_1 318198v.1